Memorandum

U.S. Department of Transportation
Office of the Secretary of Transportation

Subject: **GUIDANCE**: Interim Policies and Procedures for 49 CFR Part 15, Protection of Sensitive Security Information

Date: JUN - 7 2005

From: Vincent T. Taylor
Assistant Secretary for Administration

Reply to: Attn. of

To: Heads of Operating Administrations
Secretarial Officers

PURPOSE:

This memorandum provides interim policy and procedures, pending issuance of a final U.S. Department of Transportation (DOT) order, for the designation, maintenance, safeguarding, and disclosure of records and information that DOT or the Department of Homeland Security/Transportation Security Administration (DHS/TSA) has determined to be Sensitive Security Information (SSI).

The interim policy and procedures in this memorandum are the minimum standards for designating, marking, storing, controlling, transmitting, releasing, and destroying SSI under 49 CFR Part 15, *Protection of Sensitive Security Information*, 69 Fed. Reg. 28066 (May 18, 2004), as amended by 70 Fed. Reg. 1379 (January 7, 2005). DOT issued Part 15 concurrently with TSA's issuance of 49 CFR Part 1520, a parallel rule. On January 18, 2005 (70 Fed. Reg. 2819), DOT amended a provision of 49 CFR § 1.45 to permit delegation of SSI authority. For further reference, a current copy of 49 CFR Part 15 and 49 CFR § 1.45 is attached to this memorandum.

The Director of the Office of Intelligence, Security, and Emergency Response (S-60) is the principal policy official for SSI within DOT. The Office of the Assistant Secretary for Administration is issuing the following policy and procedures, with the concurrence of both S-60 and the Office of the General Counsel, under its authority to establish policy for the general protection of all types of sensitive information within DOT.

SENSITIVE SECURITY INFORMATION (SSI) DEFINED

"Sensitive Security Information" (SSI) is defined by 49 CFR 15.5 as sensitive but unclassified information obtained or developed in the conduct of security activities, including research and development, the unauthorized disclosure of which would be an unwarranted invasion of

privacy, reveal trade secrets or privileged information, or be detrimental to transportation safety.

Designation of information as SSI is based on the categories of information and records set forth in 49 CFR 15.5. If a specific item of information falls within one or more of the listed categories, it qualifies as SSI. For example, "security programs and contingency plans," "threat information," and "vulnerability assessments" are some of the categories listed in section 15.5(b)(1)-(15). If information fits into one of these categories, it qualifies as SSI. Section 15.5(b)(1)-(15) lists all the categories of information constituting SSI.

Each DOT operating administration should examine section 15.5(b)(1)-(15) to determine which specific information created, collected, or maintained under its purview should be designated and maintained as SSI. Information identified as SSI must be marked and safeguarded in conformity with Part 15 and the policies and procedures in this memorandum. Each operating administration should implement appropriate procedures to protect SSI.

Information designated SSI requires protection against improper disclosure, and its dissemination is restricted to authorized persons, as outlined below. Limiting access to SSI is necessary to guard against persons and entities who pose a threat to transportation security, thereby diminishing their ability to circumvent security measures. The designation of information as SSI shall be balanced against the public's legitimate interest in, and right to know, information about transportation and how its government operates.

Although SSI is subject to certain disclosure limitations, it is not classified national security information ("classified information") as defined by Executive Order 12958, *Classified National Security Information*, as amended, and is not subject to the requirements of that order. Most notably, a person does not need a security clearance in order to have access to SSI. In addition, Part 15 does not apply to information designated Critical Infrastructure Information (CII) under section 214 of the Homeland Security Act.

Finally, note that SSI is only one type of sensitive unclassified information. In general, sensitive unclassified information is information that reasonably could be expected to cause harm to government programs or facilities or to the public if improperly disclosed. Under 49 U.S.C. 40119(b)(1), information that is SSI is exempted from disclosure by exemption 3 of the Freedom of Information Act (FOIA) (records exempted from disclosure by a statute). Other sensitive unclassified information, while not covered by exemption 3 and not the subject of this memorandum, also can and should be protected from public disclosure – in some cases by using other FOIA exemptions.

ADDITIONAL DEFINITIONS

Other definitions contained in 49 CFR 15.3 that are important to the policy and procedures in this memorandum include:

- "record," which is defined as any means by which information is preserved, irrespective of format, including book, paper, drawing, map, recording, tape, film, photo, machine-

readable material, and information stored in electronic format, and includes drafts and proposed or recommended changes to a record; and

- "covered person," which is defined as any organization, entity, individual, or person, as specified in section 15.7, subject to the requirements of 49 CFR Part 15. All DOT employees are covered persons, as are contractors, grantees, consultants, licensees, and regulated entities that require access to SSI to perform work.

APPLICABILITY:

This policy and these procedures apply to all DOT employees and to all DOT contractors, grantees, consultants, licensees, and regulated entities that have access to or receive SSI. Such employees, individuals, persons, entities, and organizations are subject to the safeguarding and non-disclosure restrictions of 49 CFR Part 15 and the policy and procedures set out in this interim guidance. They are referred to as "covered persons," and that term includes all persons employed by, contracted to, or acting for a covered person, as well as persons formerly in such positions. Details regarding covered persons are set out in section 15.7.

Although not everyone will have access to SSI, everyone should be aware that some of the information that DOT manages may be SSI and must be afforded sufficient protection. Therefore, all DOT operating administrations, offices, and programs shall provide maximum distribution of this policy and procedures throughout their organizations and among all of their contractors, grantees, consultants, licensees, and regulated entities.

All DOT contracts, grants, and consulting agreements that will result in access to SSI shall include provisions for handling and protecting SSI as specified in this policy and procedures, and be consistent with 49 CFR Part 15

DELEGATIONS:

The Secretary has delegated to the Director of the Office of Intelligence, Security, and Emergency Response (S-60) the authority to establish SSI policy that is binding on all parts of DOT. In addition, the Secretary has delegated to S-60 and to the General Counsel (C-1) the authority to make SSI determinations on any matter within the purview of DOT and to resolve disputes about SSI in any part of DOT. The Secretary has also delegated to all Administrators the authority to designate information within their agency's purview as SSI. This authority may be further delegated in writing to responsible personnel within each operating administration or organization. Administrators may designate as SSI only the types of information specified in Section 15.5 (b)(1)-(15). Requests for designating information beyond the scope of 15.5 (b)(1)-(15) as SSI shall be made in writing through the Director of Intelligence, Security, and Emergency Response. Information that is pending a possible designation as SSI shall be protected as SSI until the determination has been made.

WHO MAY HAVE ACCESS TO SSI:

The standard for determining access to SSI is "need to know," which means that access to SSI is limited to authorized persons with a legitimate requirement for the information in order to

perform their official duties; carry out the requirements of a Federal contract, agreement, grant, or license; operate as a regulated entity; or perform transportation security tasks as directed by DOT. Section 15.11 specifies circumstances under which a person has the need to know. Each person with access to SSI under section 15.11 is a "covered person" under section 15.17, responsible for the maintenance and safeguarding of SSI.

In appropriate cases, DOT may further limit persons with a need to know by determining that only specific persons or classes of persons have a need to know a particular piece or category of SSI.

Having access to SSI invokes certain obligations, and a covered person has the duty to:

- protect SSI from unauthorized disclosure,
- provide access to the information only to covered persons who have a need to know,
- mark the information as specified in section 15.13 and this memorandum,
- dispose of the information as specified in section 15.19 and this memorandum, and
- report all unauthorized disclosures.

Covered persons who violate these provisions may be subject to administrative, civil, and/or criminal action for failure to properly handle or protect SSI. Section 15.9 states possible consequences of unauthorized disclosure.

DOT organizations shall ensure that the positions of all DOT employees and contractor employees having access to SSI are properly designated as to risk and sensitivity level as prescribed in DOT Order 1630.2B, Personnel Security Management. The organizations should ensure that the appropriate background investigation has been either completed or initiated before granting a DOT employee or contractor employee access to SSI. Organizations should designate as at least moderate risk those positions requiring regular SSI access.

DOT operating administrations and programs shall advise contractors, grantees, consultants, licensees, and regulated entities in writing of their obligations under Part 15 to safeguard SSI and of the penalties for unauthorized disclosure. In appropriate cases, access to SSI may be authorized subject to additional conditions, established by the Secretary of Transportation or by an Administrator.

MARKING SSI:

To ensure proper handling and protection of SSI, section 15.13 requires that it be properly marked and contain a distribution limitation statement, as specified below.

Responsibilities. A person who creates a record containing SSI or who determines that an existing record contains SSI shall, in accordance with section 15.13 and this memorandum, place or cause to be placed on the record the protective marking and limited distribution statement indicated below. A person who receives a record containing SSI that is not marked in accordance with this section shall apply such marking and inform the sender of its omission.

Protective Marking. The protective marking "**SENSITIVE SECURITY INFORMATION**" shall be applied to all records that contain SSI. On paper records, including charts, maps, and drawings, this statement should be written or stamped in plain style bold type, such as Times New Roman, and with a font size of at least 14.

Distribution Limitation Statement. The distribution limitation statement shown below shall be applied to all records that contain SSI. On paper records, including charts, maps, and drawings, this statement should be written or stamped in plain style bold type, Times New Roman and with a font size of at least 8, or an equivalent style and font size.

> **WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. Government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.**

Marking Requirements for SSI Documentation. These marking requirements apply to all records containing SSI that are created subsequent to the date of this policy memorandum, and to all existing records determined to be, in whole or in part, SSI, prior to providing access or public release.

a. Paper Records. The protective marking shall be placed conspicuously at the top of the outside of any front or back cover, on any title page, and on each page of the record. The distribution limitation statement shall be placed at the bottom of any cover, on any title page, and on each page.

b. Charts, Maps and Drawings. The protective marking and distribution limitation statement shall be affixed in a manner that makes them plainly visible.

c. Motion Picture Films, Video, and Audio Recordings.

    1) Protective Marking and Distribution Limitation Statement. The protective marking and distribution limitation statement shall be applied at the beginning and end of the medium on each reel and affixed in such a manner that it is fully visible on the screen or monitor.

    2) Motion Picture Reels. Motion picture reels that are kept in film cans or other containers shall have protective markings and distribution limitation statements applied to each side of each reel and to all sides of each can or other storage container. In addition to reproducing the protective marking and distribution limitation statement on the beginning and end portions of the film, if the motion picture film has a soundtrack, audible warnings that describe the protective marking and distribution limitation statement shall, if practicable, be included at the beginning and at the end of the film.

3) Videotape Recordings. Videotape recordings that contain SSI shall include on the recordings conspicuous visual protective markings and distribution limitation statements at both the beginning and the end, if practicable. Protective markings and the distribution limitation statement shall also be applied on the front and back and on each side of the video case and storage containers.

4) Audio Recordings. Audio recordings that contain SSI shall include on the recordings clear and conspicuous audio messages stating the protective marking and distribution limitation statement at both the beginning and the end, if practicable. Protective markings and the distribution limitation statement shall also be applied on the front and back and on each side of the audio recording case and storage containers.

d. Electronic and Magnetic Media.

1) Media Containing Information. SSI contained on electronic and magnetic media shall have protective markings and the distribution limitation statement applied at the beginning and end of the electronic and magnetic text. The protective marking and distribution limitation statement shall be displayed in such a manner that both are fully visible on a screen or monitor to anyone viewing the text. The protective marking and distribution limitation statement shall also be applied to each side of a disk and a disk sleeve/jacket, on the non-optical side of the CD-ROM, and both sides of a CD-ROM case. If the electronic/magnetic text has a soundtrack, audible warnings that describe the protective marking and distribution limitation statement shall, if possible, be included in the introduction and at the end of this text.

2) Printed Information Extracted from Media. The protective marking and distribution limitation statement may be automatically applied by the printing equipment itself on the face of a page containing SSI, provided that they are clearly distinguishable from the printed text. Information and records in the form of compiled lists shall have the protective marking affixed to the top and bottom of the first and last pages, to the top and bottom of any covers, to the top and bottom of each page containing SSI, and to the outside of the back page or cover. The distribution limitation statement shall appear on the bottom of each page containing SSI and to any cover page or back page.

Transmittal Documents. Documents that are used to transmit SSI but do not themselves contain SSI shall be marked with the protective marking and distribution limitation statement. In addition, the following statement shall be affixed to the front page of the transmittal document:

"The protective marking SENSITIVE SECURITY INFORMATION and/or the distribution limitation statement on this document are canceled when the attachments containing SSI are removed."

Portion Marking. In records containing both SSI and non-SSI data, DOT organizations shall mark only the specific portions of a record that are SSI in order to assist in the future review,

redaction, and possible release (or partial release) of the record. "SSI" shall appear in parentheses at the front of each paragraph or other portion of a document that actually contains SSI. Pictures, tables, and figures should have "SSI" in parentheses at the beginning of the associated caption. In lieu of this specific portion marking, a clarifying statement may be added to each record that identifies the SSI. Such a statement is useful where a compilation of non-sensitive information meets the criteria for designation as SSI, even though the individual items by themselves are not SSI. Non-paper records shall contain written or oral annotations attached to the media or within the content of the media to enable a reviewer to differentiate SSI material from non-SSI material. Documents that are received from organizations outside DOT and that are not portion-marked do not need to have portion marking added.

Information that is SSI for a Limited Period of Time. In some cases organizations are able to predict a future event or time after which information designated as SSI no longer warrants that designation. In such cases DOT organizations should add an additional statement with the distribution limitation statement as to the anticipated expiration date or event when the information will no longer be SSI; e.g., "The SSI designation for this information expires on [date]," or "The SSI designation for this information expires when the facility to which it pertains is closed." As with portion marking, such statements will assist in future review of records for possible release.

PROTECTING SSI:

General Requirement. All persons with access to SSI have a duty to protect it from improper disclosure; and persons with actual custody of SSI record(s) are responsible for taking reasonable steps to safeguard them and are under an affirmative duty to report any known security breaches.

Storage.

a. When a person is not in physical possession of SSI, he/she shall store it in a secure container, such as a locked desk or file cabinet, or in a locked room. SSI shall not be left exposed and unattended in areas where there is a possibility that it can be viewed by persons who do not have a need to know.

b. When an individual responsible for SSI places the material in a locked container, the individual is responsible for ensuring that positive measures are in force to restrict access to the container keys or combination to only individuals with a need to know.

c. When individuals store SSI on computers, including portable computing devices, they should carefully safeguard the equipment at all times when it is not stored in a locked container or room. They should use passwords to protect SSI and exercise proper care in protecting any storage medium (e.g., CD-ROM or other disk) containing it.

Packing and Transmission.

General. When assembling a package containing SSI for transmission, it is the responsibility of the individual preparing the package to ensure that all SSI has the appropriate protective markings and distribution limitation statements.

a. Mail. SSI may be transmitted by U.S. Postal Service first class mail or regular parcel post, or by commercial delivery services (Federal Express, UPS, etc). SSI that is to be sent by mail or by a delivery service shall be wrapped in opaque envelopes, wrappings, or cartons. The mail should be addressed only to a person or position who the sender is reasonably sure is a covered person with a need to know. The outside of the package or envelope shall contain a notation that it is to be opened only by the addressee.

b. Interoffice mail. When sent by interoffice mail, SSI shall be transmitted in a sealed envelope in such a manner as to prevent inadvertent visual disclosure. The outside of the package or envelope shall contain a notation that it is to be opened only by the addressee.

c. Hand carrying within or between buildings. SSI that is carried by hand within or between buildings shall be protected (by a cover sheet, briefcase, protective folder, distribution pouch, etc.) to prevent inadvertent visual disclosure.

d. Packaging material. Envelopes or containers shall be of such strength and durability that they provide physical protection during transit and prevent items from breaking out of the containers or envelopes.

e. Electronic Mail (e-mail). SSI transmitted via e-mail shall be in a password-protected attachment. The password shall be communicated to the recipient by means other than the text of the e-mail.

f. Web Posting. DOT organizations, contractors, grantees, consultants, licensees and regulated entities should be especially careful to ensure that no SSI is available on any internet or intranet site, except for postings on secure sites where all persons with access have a need to know the SSI.

g. Facsimile. When sending SSI via facsimile, the sender should confirm that the fax number of the recipient is current and valid and should ensure that either the intended recipient is present to promptly receive the fax or that the receiving fax machine is in a controlled area where unauthorized persons will not have access to it. Fax transmittal sheets should be used that describe the sensitivity of the contents and provide instructions in the event the fax is received by someone other than the intended person.

h. Telephone. A person providing SSI via the telephone shall ensure that the person receiving the SSI is an authorized recipient. The risk of interception and monitoring of conversations is greater when using cellular telephones and when using cordless telephones, which transmit the conversation to a base unit. Individuals needing to pass SSI by telephone shall avoid these devices unless the circumstances are exigent or the transmissions are encoded or otherwise protected. Secure communications equipment is ideal for transmitting SSI.

i. Conversations. SSI may be discussed in offices or other locations where the parties to the conversation are reasonably sure that the conversations cannot be overheard by anyone without a need to know.

j. DOT organizations shall ensure that the contents of Sections 15.7, 15.9, and 15.11, including the above measures for the protection of SSI and the disclosure limitations, are communicated to all contractors, grantees, consultants, licensees, and regulated entities that employ or may employ, "covered persons" before such covered persons have access to SSI.

RETENTION/DESTRUCTION OF SSI:

a. DOT personnel may be required to retain some SSI information under Federal record retention laws. SSI not subject to such requirements may be destroyed when no longer needed to carry out agency functions or transportation safety measures.

b. Other covered persons, including DOT contractors, grantees, consultants, and regulated entities, are not authorized to retain SSI permanently and should destroy it when no longer required to carry out their work or project. All contracts and agreements for work that require or may require access to or custody of SSI shall specify that at the conclusion of work the other covered persons shall either destroy or return to DOT all SSI that was obtained or prepared as the result of work under the contract or agreement. However, State and local governments are not required to destroy SSI if the records must be preserved under State or local law.

c. Destruction may be by shredding, burning, pulping or any other method to make the information unrecognizable and preclude its reconstruction. For paper records, tearing in half is not a sufficient means of destroying SSI. Existing strip shredders may be used, but any new shredding equipment shall employ a cross-cut feature. For large records, only portions that actually contain SSI must be destroyed in this manner. Any other pages being disposed of in a normal manner should first have the SSI annotations marked out. It is acceptable to dispose of SSI in containers that are designed to accept it and where it will be disposed of properly under controlled conditions.

DISCLOSURE, CONTROL, AND RELEASE OF SSI:

In general, records containing SSI are not available for public inspection or copying, and release of SSI is limited to persons or entities with a need to know the information.

a. Except as provided in this memorandum, the authority to release SSI to persons who are not otherwise eligible, such as individual Members of Congress, is limited to S-60, with the concurrence of the Office of the General Counsel (C).

b. A covered person may disclose SSI only to another covered person with a need to know, with certain exceptions listed in Section 15.15. Unauthorized disclosures of SSI are subject to civil penalty, administrative action, or, in appropriate cases, criminal prosecution. Authorized access to SSI shall be accompanied by an explanation, which may be oral, of the restrictions that apply to the use and further dissemination of the SSI, and the penalties for improper use or dissemination. Access shall be denied if the recipient indicates an inability or unwillingness to abide by the restrictions.

c. Requests by non-covered persons for SSI should normally be denied or referred to the applicable component or agency within DOT or the Department of Homeland Security (DHS) if DHS originated the SSI designation.

d. DOT employees and all other covered persons shall promptly report in writing any instances where SSI has been released to unauthorized persons. DOT organizations shall identify a point of contact to receive and process such reports and shall ensure that all covered persons know how to report the information. The point of contact shall inform S-60 and the Director, Office of Security (M-40), in writing of all unauthorized releases of SSI information. S-60 will ensure that the originating organization is aware of the release. M-40 will be responsible for conducting and/or coordinating investigations of all such alleged instances within DOT and its contractors, grantees, consultants, licensees, and regulated entities.

e. Disclosure of SSI to a foreign government and/or other foreign or international entity shall be approved by S-60 upon the request of the DOT operating administration or program or the contractor, grantee, consultant, licensee, or regulated entity in possession of the SSI.

f. Disclosure of SSI to committees of Congress, the Government Accountability Office (GAO), and the Comptroller General is authorized without prior approval, but shall be reported to S-60. Any such release shall comply with all elements of this guidance, including the marking and distribution limitation statement requirements. In addition, any release to GAO or the Comptroller General requires concurrence by the Departmental Audit Liaison, M-1. Any other release of SSI to non-covered persons or entities shall have prior approval of S-60, with the concurrence of C. Requests may be made through the originating organization.

g. Freedom of Information Act (FOIA) Requests. Records and information determined to be SSI under Part 15 are exempt from public disclosure under FOIA pursuant to exemption 3 (5 U.S.C. 552(b)(3)), although reasonably segregable, non-SSI portions of the record must be disclosed.

   1) Authority to deny FOIA requests. FOIA requests for SSI are processed by the appropriate DOT agency/entity (see 49 CFR Part 7), except that any decision to release SSI shall have the concurrence of the Chief Counsel of the affected operating administration and the General Counsel.

   2) Information requests received by regulated parties. Requests for SSI that are addressed to regulated parties, such as under State or local freedom of information or open records acts, are addressed in 49 CFR section 15.15.

   3) Release of records containing both SSI and non-SSI. If a record contains information exempt from disclosure under part 15 but also contains information that may be disclosed, the latter information will be provided in response to a FOIA request, provided the record is not otherwise exempt from disclosure under FOIA, if it is

practical to redact the requested information from the record. Records from which information has been redacted will so indicate by a legible statement in the margin indicating redaction under the authority of Part 15. If it is not practical to redact SSI, the entire record will be withheld from public disclosure

h. Enforcement Proceedings. Access to SSI may be provided in enforcement proceedings when, in the sole discretion of the Secretary of Transportation, access is necessary for responding to enforcement allegations or to serve the interests of justice.

i. Rulemaking. Information submitted to a DOT rulemaking docket that is claimed by the submitter, or determined by DOT, to be SSI shall be handled as follows:

1) A copy of the docket submission noting where the SSI information is located, but without the SSI information itself, shall be filed in the docket.

2) A copy of the docket submission noting where the SSI information is located and including the SSI information shall be filed in a sealed envelope that complies with the handling instructions above and includes on its outer surface the number of the docket to which it is being submitted and the identity of the submitter.

j. Critical Infrastructure Information (CII). Disclosure of information that is both SSI and as CII under section 214 of the Homeland Security Act is governed solely by the requirements of section 214 and any implementing regulations.

If you have any questions, please contact Richard Thompson in the Office of Security (M-40) at 202-366-4678; or Bob Ross, Office of the General Counsel, at 202-366-9156.

Attachment

49 CFR Part 15

TITLE 49--TRANSPORTATION

Subtitle A--Office of the Secretary of Transportation

PART 15. PROTECTION OF SENSITIVE SECURITY INFORMATION--Table of Contents

Sec. 15.1 Scope.

(a) Applicability. This part governs the maintenance, safeguarding, and disclosure of records and information that the Secretary of DOT has determined to be Sensitive Security Information, as defined in Sec. 15.5. This part does not apply to the maintenance, safeguarding, or disclosure of classified national security information, as defined by Executive Order 12968, or to other sensitive unclassified information that is not SSI, but that nonetheless may be exempt from public disclosure under the Freedom of Information Act. In addition, in the case of information that has been designated as critical infrastructure information under section 214 of the Homeland Security Act, the receipt, maintenance, or disclosure of such information by a Federal agency or employee is governed by section 214 and any implementing regulations, not by this part.

(b) Delegation. The authority of the Secretary under this part may be further delegated within DOT.

Sec. 15.3 Terms used in this part.

In addition to the terms in Sec. 15.3 of this chapter, the following terms apply in this part:

Administrator means the Under Secretary of Transportation for Security referred to in 49 U.S.C. 114(b), or his or her designee.

Coast Guard means the United States Coast Guard.

Covered person means any organization, entity, individual, or other person described in Sec. 15.7. In the case of an individual, covered person includes any individual applying for employment in a position that would be a covered person, or in training for such a position, regardless of whether that individual is receiving a wage, salary, or other form of payment. Covered person includes a person applying for certification or other form of approval that, if granted, would make the person a covered person described in Sec. 15.7.

DHS means the Department of Homeland Security and any directorate, bureau, or other component within the Department of Homeland Security, including the United States Coast Guard.

DOT means the Department of Transportation and any operating administration, entity, or office within the Department of Transportation, including the Saint Lawrence Seaway Development Corporation and the Bureau of Transportation Statistics.

Federal Flight Deck Officer means a pilot participating in the Federal Flight Deck Officer Program under 49 U.S.C. 44921 and implementing regulations.

Maritime facility means any facility as defined in 33 CFR part 101.

Record includes any means by which information is preserved, irrespective of format, including a book, paper, drawing, map, recording, tape, film, photograph, machine-readable material, and any information stored in an electronic format. The term record also includes any draft, proposed, or recommended change to any record.

Security contingency plan means a plan detailing response procedures to address a transportation security incident, threat assessment, or specific threat against transportation, including details of preparation, response, mitigation, recovery, and reconstitution procedures, continuity of government, continuity of transportation operations, and crisis management.

Security program means a program or plan and any amendments developed for the security of the following, including any comments, instructions, or implementing guidance:

(1) An airport, aircraft, or aviation cargo operation;

(2) A maritime facility, vessel, or port area; or

(3) A transportation-related automated system or network for information processing, control, and communications.

Security screening means evaluating a person or property to determine whether either poses a threat to security.

SSI means sensitive security information, as described in Sec. 15.5.

Threat image projection system means an evaluation tool that involves periodic presentation of fictional threat images to operators and is used in connection with x-ray or explosives detection systems equipment.

TSA means the Transportation Security Administration.

Vulnerability assessment means any review, audit, or other examination of the security of a transportation infrastructure asset; airport; maritime facility, port area, vessel, aircraft, train, commercial motor vehicle, or pipeline, or a transportation-related automated system or network, to determine its vulnerability to unlawful interference, whether during the conception, planning, design, construction, operation, or decommissioning phase. A vulnerability assessment may include proposed, recommended, or directed actions or countermeasures to address security concerns.

Sec. 15.5 Sensitive security information.

(a) In general. In accordance with 49 U.S.C. 40119(b)(1), SSI is information obtained or developed in the conduct of security activities, including research and development, the disclosure of which the Secretary of DOT has determined would--

(1) Constitute an unwarranted invasion of privacy (including, but not limited to, information contained in any personnel, medical, or similar file);

(2) Reveal trade secrets or privileged or confidential information obtained from any person; or

(3) Be detrimental to transportation safety.

(b) Information constituting SSI. Except as otherwise provided in writing by the Secretary of DOT in the interest of public safety or in furtherance of transportation security, the following information, and records containing such information, constitute SSI:

(1) Security programs and contingency plans. Any security program or security contingency plan issued, established, required, received, or approved by DOT or DHS, including--

(i) Any aircraft operator or airport operator security program or security contingency plan under this chapter;

(ii) Any vessel, maritime facility, or port area security plan required or directed under Federal law;

(iii) Any national or area security plan prepared under 46 U.S.C. 70103; and

(iv) Any security incident response plan established under 46 U.S.C. 70104.

(2) Security Directives. Any Security Directive or order--

(i) Issued by TSA under 49 CFR 1542.303, 1544.305, or other authority;

(ii) Issued by the Coast Guard under the Maritime Transportation Security Act, 33 CFR part 6, or 33 U.S.C. 1221 et seq. related to maritime security; or

(iii) Any comments, instructions, and implementing guidance pertaining thereto.

(3) Information Circulars. Any notice issued by DHS or DOT regarding a threat to aviation or maritime transportation, including any--

(i) Information Circular issued by TSA under 49 CFR 1542.303 or 1544.305, or other authority; and

(ii) Navigation or Vessel Inspection Circular issued by the Coast Guard related to maritime security.

(4) Performance specifications. Any performance specification and any description of a test object or test procedure, for--

(i) Any device used by the Federal government or any other person pursuant to any aviation or maritime transportation security requirements of Federal law for the detection of any weapon, explosive, incendiary, or destructive device or substance; and

(ii) Any communications equipment used by the Federal government or any other person in carrying out or complying with any aviation or maritime transportation security requirements of Federal law.

(5) Vulnerability assessments. Any vulnerability assessment directed, created, held, funded, or approved by the DOT, DHS, or that will be provided to DOT or DHS in support of a Federal security program.

(6) Security inspection or investigative information. (i) Details of any security inspection or investigation of an alleged violation of aviation or maritime transportation security requirements of Federal law that could reveal a security vulnerability, including the identity of the Federal special agent or other Federal employee who conducted the inspection or audit.

(ii) In the case of inspections or investigations performed by TSA, this includes the following information as to events that occurred within 12 months of the date of release of the information: the name of the airport where a violation occurred, the airport identifier in the case number, a description of the violation, the regulation allegedly violated, and the identity of any aircraft operator in connection with specific locations or specific security procedures. Such information will be released after the relevant 12-month period, except that TSA

will not release the specific gate or other location on an airport where an event occurred, regardless of the amount of time that has passed since its occurrence. During the period within 12 months of the date of release of the information, TSA may release summaries of an aircraft operator's, but not an airport operator's, total security violations in a specified time range without identifying specific violations or locations. Summaries may include total enforcement actions, total proposed civil penalty amounts, number of cases opened, number of cases referred to TSA or FAA counsel for legal enforcement action, and number of cases closed.

(7) Threat information. Any information held by the Federal government concerning threats against transportation or transportation systems and sources and methods used to gather or develop threat information, including threats against cyber infrastructure.

(8) Security measures. Specific details of aviation or maritime transportation security measures, both operational and technical, whether applied directly by the Federal government or another person, including--

(i) Security measures or protocols recommended by the Federal government;

(ii) Information concerning the deployments, numbers, and operations of Coast Guard personnel engaged in maritime security duties and Federal Air Marshals, to the extent it is not classified national security information; and

(iii) Information concerning the deployments and operations of Federal Flight Deck Officers, and numbers of Federal Flight Deck Officers aggregated by aircraft operator.

(9) Security screening information. The following information regarding security screening under aviation or maritime transportation security requirements of Federal law:

(i) Any procedures, including selection criteria and any comments, instructions, and implementing guidance pertaining thereto, for screening of persons, accessible property, checked baggage, U.S. mail, stores, and cargo, that is conducted by the Federal government or any other authorized person.

(ii) Information and sources of information used by a passenger or property screening program or system, including an automated screening system.

(iii) Detailed information about the locations at which particular screening methods or equipment are used, only if determined by TSA to be SSI.

(iv) Any security screener test and scores of such tests.

(v) Performance or testing data from security equipment or screening systems.

(vi) Any electronic image shown on any screening equipment monitor, including threat images and descriptions of threat images for threat image projection systems.

(10) Security training materials. Records created or obtained for the purpose of training persons employed by, contracted with, or acting for the Federal government or another person to carry out any aviation or maritime transportation security measures required or recommended by DHS or DOT.

(11) Identifying information of certain transportation security personnel. (i) Lists of the names or other identifying information that identify persons as--

(A) Having unescorted access to a secure area of an airport or a

secure or restricted area of a maritime facility, port area, or vessel or;

(B) Holding a position as a security screener employed by or under contract with the Federal government pursuant to aviation or maritime transportation security requirements of Federal law, where such lists are aggregated by airport;

(C) Holding a position with the Coast Guard responsible for conducting vulnerability assessments, security boardings, or engaged in operations to enforce maritime security requirements or conduct force protection;

(D) Holding a position as a Federal Air Marshal; or

(ii) The name or other identifying information that identifies a person as a current, former, or applicant for Federal Flight Deck Officer.

(12) Critical aviation or maritime infrastructure asset information. Any list identifying systems or assets, whether physical or virtual, so vital to the aviation or maritime transportation system that the incapacity or destruction of such assets would have a debilitating impact on transportation security, if the list is--

(i) Prepared by DHS or DOT; or

(ii) Prepared by a State or local government agency and submitted by the agency to DHS or DOT.

(13) Systems security information. Any information involving the security of operational or administrative data systems operated by the Federal government that have been identified by the DOT or DHS as critical to aviation or maritime transportation safety or security, including automated information security procedures and systems, security inspections, and vulnerability information concerning those systems.

(14) Confidential business information. (i) Solicited or unsolicited proposals received by DHS or DOT, and negotiations arising therefrom, to perform work pursuant to a grant, contract, cooperative agreement, or other transaction, but only to the extent that the subject matter of the proposal relates to aviation or maritime transportation security measures;

(ii) Trade secret information, including information required or requested by regulation or Security Directive, obtained by DHS or DOT in carrying out aviation or maritime transportation security responsibilities; and

(iii) Commercial or financial information, including information required or requested by regulation or Security Directive, obtained by DHS or DOT in carrying out aviation or maritime transportation security responsibilities, but only if the source of the information does not customarily disclose it to the public.

(15) Research and development. Information obtained or developed in the conduct of research related to aviation or maritime transportation security activities, where such research is approved, accepted, funded, recommended, or directed by the DHS or DOT, including research results.

(16) Other information. Any information not otherwise described in this section that TSA determines is SSI under 49 U.S.C. 114(s) or that the Secretary of DOT determines is SSI under 49 U.S.C. 40119. Upon the request of another Federal agency, the Secretary of DOT may designate as SSI information not otherwise described in this section.

(c) Loss of SSI designation. The Secretary of DOT may determine in writing that information or records described in paragraph (b) of this section do not constitute SSI because they no longer meet the criteria

set forth in paragraph (a) of this section.

Sec. 15.7 Covered persons.

Persons subject to the requirements of part 15 are:

(a) Each airport operator and aircraft operator subject to the requirements of Subchapter C of this title.

(b) Each indirect air carrier, as defined in 49 CFR 1540.5.

(c) Each owner, charterer, or operator of a vessel, including foreign vessel owners, charterers, and operators, required to have a security plan under Federal or International law.

(d) Each owner or operator of a maritime facility required to have a security plan under the Maritime Transportation Security Act, (Pub. L. 107-295), 46 U.S.C. 70101 et seq., 33 CFR part 6, or 33 U.S.C. 1221 et seq.

(e) Each person performing the function of a computer reservation system or global distribution system for airline passenger information.

(f) Each person participating in a national or area security committee established under 46 U.S.C. 70112, or a port security committee.

(g) Each industry trade association that represents covered persons and has entered into a non-disclosure agreement with the DHS or DOT.

(h) DHS and DOT.

(i) Each person conducting research and development activities that relate to aviation or maritime transportation security and are approved, accepted, funded, recommended, or directed by DHS or DOT.

(j) Each person who has access to SSI, as specified in Sec. 15.11.

(k) Each person employed by, contracted to, or acting for a covered person, including a grantee of DHS or DOT, and including a person formerly in such position.

(l) Each person for which a vulnerability assessment has been directed, created, held, funded, or approved by the DOT, DHS, or that has prepared a vulnerability assessment that will be provided to DOT or DHS in support of a Federal security program.

(m) Each person receiving SSI under Sec. 1520.15(d) or (e).

Sec. 15.9 Restrictions on the disclosure of SSI.

(a) Duty to protect information. A covered person must--

(1) Take reasonable steps to safeguard SSI in that person's possession or control from unauthorized disclosure. When a person is not in physical possession of SSI, the person must store it a secure container, such as a locked desk or file cabinet or in a locked room.

(2) Disclose, or otherwise provide access to, SSI only to covered persons who have a need to know, unless otherwise authorized in writing by TSA, the Coast Guard, or the Secretary of DOT.

(3) Refer requests by other persons for SSI to TSA or the applicable component or agency within DOT or DHS.

(4) Mark SSI as specified in Sec. 15.13.

(5) Dispose of SSI as specified in Sec. 15.19.

(b) Unmarked SSI. If a covered person receives a record containing SSI that is not marked as specified in Sec. 1520.13, the covered person must--

(1) Mark the record as specified in Sec. 15.13; and

(2) Inform the sender of the record that the record must be marked as specified in Sec. 15.13.

(c) Duty to report unauthorized disclosure. When a covered person becomes aware that SSI has been released to unauthorized persons, the covered person must promptly inform TSA or the applicable DOT or DHS component or agency.

(d) Additional requirements for critical infrastructure information. In the case of information that is both SSI and has been designated as critical infrastructure information under section 214 of the Homeland Security Act, any covered person who is a Federal employee in possession of such information must comply with the disclosure restrictions and other requirements applicable to such information under section 214 and any implementing regulations.

Sec. 15.11 Persons with a need to know.

(a) In general. A person has a need to know SSI in each of the following circumstances:

(1) When the person requires access to specific SSI to carry out transportation security activities approved, accepted, funded, recommended, or directed by DHS or DOT.

(2) When the person is in training to carry out transportation security activities approved, accepted, funded, recommended, or directed by DHS or DOT.

(3) When the information is necessary for the person to supervise or otherwise manage individuals carrying out transportation security activities approved, accepted, funded, recommended, or directed by the DHS or DOT.

(4) When the person needs the information to provide technical or legal advice to a covered person regarding transportation security requirements of Federal law.

(5) When the person needs the information to represent a covered person in connection with any judicial or administrative proceeding regarding those requirements.

(b) Federal employees, contractors, and grantees. (1) A Federal employee has a need to know SSI if access to the information is necessary for performance of the employee's official duties.

(2) A person acting in the performance of a contract with or grant from DHS or DOT has a need to know SSI if access to the information is necessary to performance of the contract or grant.

(c) Background check. The Secretary of DOT may make an individual's access to the SSI contingent upon satisfactory completion of a security background check and the imposition of procedures and requirements for safeguarding SSI that are satisfactory to the Secretary.

(d) Need to know further limited by the DHS or DOT. For some specific SSI, DHS or DOT may make a finding that only specific persons or classes of persons have a need to know.

Sec. 15.13 Marking SSI.

(a) Marking of paper records. In the case of paper records containing SSI, a covered person must mark the record by placing the protective marking conspicuously on the top, and the distribution limitation statement on the bottom, of--

(1) The outside of any front and back cover, including a binder cover or folder, if the document has a front and back cover;

(2) Any title page; and

(3) Each page of the document.

(b) Protective marking. The protective marking is: SENSITIVE SECURITY INFORMATION.

(c) Distribution limitation statement. The distribution limitation statement is:

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a ``need to know'', as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

(d) Other types of records. In the case of non-paper records that contain SSI, including motion picture films, videotape recordings, audio recording, and electronic and magnetic records, a covered person must clearly and conspicuously mark the records with the protective marking and the distribution limitation statement such that the viewer or listener is reasonably likely to see or hear them when obtaining access to the contents of the record.

Sec. 15.15 SSI disclosed by DOT.

(a) In general. Except as otherwise provided in this section, and notwithstanding the Freedom of Information Act (5 U.S.C. 552), the Privacy Act (5 U.S.C. 552a), and other laws, records containing SSI are not available for public inspection or copying, nor does DOT release such records to persons without a need to know.

(b) Disclosure under the Freedom of Information Act and the Privacy Act. If a record contains both SSI and information that is not SSI, DOT, on a proper Freedom of Information Act or Privacy Act request, may disclose the record with the SSI redacted, provided the record is not otherwise exempt from disclosure under the Freedom of Information Act or Privacy Act.

(c) Disclosures to committees of Congress and the General Accounting Office. Nothing in this part precludes DOT from disclosing SSI to a committee of Congress authorized to have the information or to the Comptroller General, or to any authorized representative of the Comptroller General.

(d) Disclosure in enforcement proceedings. (1) In general. The Secretary of DOT may provide SSI to a person in the context of an administrative enforcement proceeding when, in the sole discretion of the Secretary, access to the SSI is necessary for the person to prepare a response to allegations contained in a legal enforcement action document issued by DOT.

(2) Security background check. Prior to providing SSI to a person under paragraph (d)(1) of this section, the Secretary of DOT may require the individual or, in the case of an entity, the individuals representing the entity, and their counsel, to undergo and satisfy, in the judgment of the Secretary of DOT, a security background check.

(e) Other conditional disclosure. The Secretary of DOT may authorize a conditional disclosure of specific records or information that constitute SSI upon the written determination by the Secretary that disclosure of such records or information, subject to such limitations and restrictions as the Secretary may prescribe, would not be detrimental to transportation safety.

(f) Obligation to protect information. When an individual receives

SSI pursuant to paragraph (d) or (e) of this section that individual becomes a covered person under Sec. 15.7 and is subject to the obligations of a covered person under this part.

(g) No release under FOIA. When DOT discloses SSI pursuant to paragraphs (b) through (e) of this section, DOT makes the disclosure for the sole purpose described in that paragraph. Such disclosure is not a public release of information under the Freedom of Information Act.

(h) Disclosure of Critical Infrastructure Information. Disclosure of information that is both SSI and has been designated as critical infrastructure information under section 214 of the Homeland Security Act is governed solely by the requirements of section 214 and any implementing regulations.

Sec. 15.17 Consequences of unauthorized disclosure of SSI.

Violation of this part is grounds for a civil penalty and other enforcement or corrective action by DOT, and appropriate personnel actions for Federal employees. Corrective action may include issuance of an order requiring retrieval of SSI to remedy unauthorized disclosure or an order to cease future unauthorized disclosure.

Sec. 15.19 Destruction of SSI.

(a) DOT. Subject to the requirements of the Federal Records Act (5 U.S.C. 105), including the duty to preserve records containing documentation of a Federal agency's policies, decisions, and essential transactions, DOT destroys SSI when no longer needed to carry out the agency's function.

(b) Other covered persons. (1) In general. A covered person must destroy SSI completely to preclude recognition or reconstruction of the information when the covered person no longer needs the SSI to carry out transportation security measures.

(2) Exception. Paragraph (b)(1) of this section does not require a State or local government agency to destroy information that the agency is required to preserve under State or local law.

****

CODE OF FEDERAL REGULATIONS

TITLE 49--TRANSPORTATION

SUBTITLE A--OFFICE OF THE SECRETARY OF TRANSPORTATION

PART 1--ORGANIZATION AND DELEGATION OF POWERS AND DUTIES

SUBPART C--DELEGATIONS

§ 1.45 Delegations to all Administrators.

(19) Carry out the functions vested in the Secretary by 49 U.S.C. 40119(b), as implemented by 49 CFR part 15, relating to the determination that information is Sensitive Security Information within their respective organizations.

(b) Except as otherwise specifically provided, each official to whom authority is granted by §§ 1.45 through 1.53, 1.66, and 1.68 may redelegate and authorize successive redelegations of that authority within the organization under that official's jurisdiction.